



27123

PATENT TRADEMARK OFFICE

Docket No. 1232-4812

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant(s): Masashi HAMADA

Group Art Unit:

Serial No.: 10/057,255

Examiner:

Filed: January 24, 2002

For: DATA MANAGEMENT METHOD USING NETWORK

CLAIM TO CONVENTION PRIORITY

Commissioner for Patents
Washington, D.C. 20231

RECEIVED
APR 17 2002
Technology Center 2100

Sir:

In the matter of the above-identified application and under the provisions of 35 U.S.C. §119 and 37 C.F.R. §1.55, applicant(s) claim(s) the benefit of the following prior application(s):

Application(s) filed in: Japan
In the name of: Canon Kabushiki Kaisha

Serial No(s): 2001-021657
Filing Date(s): January 30, 2001

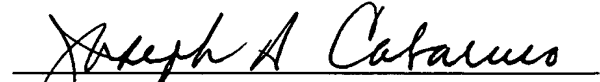
Serial No(s): 2001-193446
Filing Date(s): June 26, 2001

- ☒ Pursuant to the Claim to Priority, applicant(s) submit(s) a duly certified copy of said foreign application.
- ☐ A duly certified copy of said foreign application is in the file of application Serial No. _____, filed _____.

Respectfully submitted,
MORGAN & FINNEGAN, L.L.P.

Dated: April 7, 2002

By:


Joseph A. Calvaruso
Registration No. 28,287

Correspondence Address:

MORGAN & FINNEGAN, L.L.P.
345 Park Avenue
New York, NY 10154-0053
(212) 758-4800 Telephone
(212) 751-6849 Facsimile



(translation of the front page of the priority document of
Japanese Patent Application No. 2001-021657)

JAPAN PATENT OFFICE

This is to certify that the annexed is a true copy of the
following application as filed with this Office.

RECEIVED
APR 17 2002
Technology Center 2100

Date of Application: January 30, 2001

Application Number : Patent Application 2001-021657

[ST.10/C] : [JP 2001-021657]

Applicant(s) : Canon Kabushiki Kaisha

February 22, 2002

Commissioner,

Japan Patent Office

Kouzo OIKAWA

Certification Number 2002-3009882

CFM 2495 US

日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出 願 年 月 日
Date of Application: 2001年 1月30日

出 願 番 号
Application Number: 特願2001-021657

[ST.10/C]: [JP2001-021657]

出 願 人
Applicant(s): キヤノン株式会社

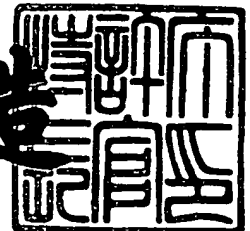
RECEIVED
APR 17 2002
Technology Center 2100

CERTIFIED COPY OF
PRIORITY DOCUMENT

2002年 2月22日

特 許 庁 長 官
Commissioner,
Japan Patent Office

及 川 耕 造



【書類名】 特許願

【整理番号】 4221036

【提出日】 平成13年 1月30日

【あて先】 特許庁長官殿

【国際特許分類】 G06F 15/00

【発明の名称】 データ管理方法

【請求項の数】 14

【発明者】

 【住所又は居所】 東京都大田区下丸子3丁目30番2号 キヤノン株式会社
社内

 【氏名】 浜田 正志

【特許出願人】

 【識別番号】 000001007

 【氏名又は名称】 キヤノン株式会社

【代理人】

 【識別番号】 100076428

 【弁理士】

 【氏名又は名称】 大塚 康德

 【電話番号】 03-5276-3241

【選任した代理人】

 【識別番号】 100115071

 【弁理士】

 【氏名又は名称】 大塚 康弘

 【電話番号】 03-5276-3241

【手数料の表示】

 【予納台帳番号】 003458

 【納付金額】 21,000円

【提出物件の目録】

 【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 0001010

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 データ管理方法

【特許請求の範囲】

【請求項 1】 サーバとクライアント端末とを含むネットワークシステムを利用したデータ管理方法であって、

サーバにより、クライアント端末からの利用者によるデータ格納要求を受け付ける受付工程と、

前記サーバにより、前記利用者が設定した地域と一定の関係のある地域に設置されたデータサーバを選定する選定工程と、

前記サーバにより、選定した前記データサーバに、前記データ格納要求に係るデータを送信し、格納させる格納工程と、
を含むデータ管理方法。

【請求項 2】 前記選定工程では、

前記サーバにより、少なくとも、前記利用者が設定した地域以外の地域に設置された前記データサーバを選定することを特徴とする請求項 1 に記載のデータ管理方法。

【請求項 3】 前記選定工程では、

前記サーバにより、前記データサーバを複数選定し、

前記格納工程では、

選定した各々の前記データサーバに、前記データ格納要求に係るデータを送信し、格納させることを特徴とする請求項 1 に記載のデータ管理方法。

【請求項 4】 更に、

前記サーバにより、災害情報を提供する災害情報データベースから災害情報を取得し、取得した前記災害情報に基づいて、災害発生率の低い地域を検索する工程を含み、

前記選定工程では、

前記サーバにより、少なくとも、前記利用者が設定した地域以外の地域に設置された前記データサーバと、前記災害発生率の低い地域に設置された前記データサーバと、を選定することを特徴とする請求項 3 に記載のデータ管理方法。

【請求項 5】 更に、

前記サーバにより、前記データ格納要求に係るデータを暗号化する工程を含み

前記サーバにより、各々の前記データサーバに対して、それぞれ異なる手法により暗号化された前記データを送信し、格納させることを特徴とする請求項 3 に記載のデータ管理方法。

【請求項 6】 更に、

前記サーバにより、各々の前記データサーバから、定期的に、暗号化された前記データを取得する工程と、

前記サーバにより、取得した前記データをそれぞれ復号化する工程と、

前記サーバにより、復号化した前記データを、それぞれ比較する工程と、を含むことを特徴とする請求項 5 に記載のデータ管理方法。

【請求項 7】 更に、

前記サーバにより、前記データを格納した前記データサーバのアドレスを、前記クライアント端末に送信する工程を含むことを特徴とする請求項 1 に記載のデータ管理方法。

【請求項 8】 更に、

前記サーバにより、前記データを格納した前記データサーバのアドレスと、暗号化された前記データを復号化するためのキーと、を、前記クライアント端末に送信する工程を含むことを特徴とする請求項 5 に記載のデータ管理方法。

【請求項 9】 前記利用者が設定した地域の情報は、予め前記サーバに格納されていることを特徴とする請求項 1 に記載のデータ管理方法。

【請求項 10】 更に、

前記データサーバにより、前記クライアント端末からの利用者によるデータ送信要求を受け付ける工程と、

前記データサーバにより、前記データ送信要求に係るデータを、前記クライアント端末に送信する工程と、

を含むことを特徴とする請求項 1 に記載のデータ管理方法。

【請求項 11】 サーバとクライアント端末とを含むネットワークシステム

を利用したデータ管理方法であって、

サーバにより、クライアント端末からの利用者によるデータ格納要求を受け付ける受付工程と、

前記サーバにより、前記データ格納要求に係るデータを格納するデータサーバを選定する選定工程と、

前記サーバにより、選定した前記データサーバに、前記データ格納要求に係るデータを送信し、格納させる格納工程と、

を含むデータ管理方法。

【請求項12】 通信回線を介してクライアント端末から送信された、利用者によるデータ格納要求を受け付ける受付手段と、

前記データ格納要求に係るデータを格納するデータサーバを選定する選定手段と、

選定した前記データサーバに、通信回線を介して前記データ格納要求に係るデータを送信する手段と、

を備えたことを特徴とするサーバ。

【請求項13】 コンピュータを、

通信回線を介してクライアント端末から送信された、利用者によるデータ格納要求を受け付ける受付手段、

前記データ格納要求に係るデータを格納するデータサーバを選定する選定手段

、
選定した前記データサーバに、通信回線を介して前記データ格納要求に係るデータを送信する手段、

として機能させるプログラム。

【請求項14】 相互に通信回線を介して通信可能とされた統括サーバ、クライアント端末、及び、複数のデータサーバを含むデータ管理システムであって、

前記統括サーバが、

前記クライアント端末から送信された、利用者によるデータ格納要求を受け付ける受付手段と、

前記データサーバの中から、前記データ格納要求に係るデータを格納するデータサーバを選定する選定手段と、

選定した前記データサーバに、前記データ格納要求に係るデータを送信する手段と、を備え、

前記データサーバが、

前記統括サーバから送信された前記データを格納する手段を備えたことを特徴とするデータ管理システム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、データ管理技術に関し、特に、ユーザが所有するデータをネットワークを利用して管理する技術に関する。

【0002】

【従来の技術】

従来、ユーザが作成し、又は、取得した電子写真やビデオストリーム等のデータは、広く公開することを目的としない限り、そのユーザが所有するパソコン等の大容量ハードディスクやDVD、CD-R等でローカルに格納されていた。

【0003】

【発明が解決しようとする課題】

しかしながら、例えば、携帯型端末等によって、容量が大きなデータを得た場合には、そのデータにより携帯型端末等のメモリが占有されてしまい、他のデータを格納するメモリ領域が少なくなるという問題がある。

【0004】

また、パーソナルコンピュータ等にユーザが作成したデータを格納する場合であっても、その設置場所が火災・地震・台風等の災害に被災した場合、大切なデータが失われる恐れもあった。

【0005】

従って、本発明の目的は、ユーザが所有する電子データを好適に管理するデータ管理技術を提供することにある。

【0006】

【課題を解決するための手段】

本発明によれば、サーバとクライアント端末とを含むネットワークシステムを利用したデータ管理方法であって、

サーバにより、クライアント端末からの利用者によるデータ格納要求を受け付ける受付工程と、

前記サーバにより、前記利用者が設定した地域と一定の関係のある地域に設置されたデータサーバを選定する選定工程と、

前記サーバにより、選定した前記データサーバに、前記データ格納要求に係るデータを送信し、格納させる格納工程と、

を含むデータ管理方法が提供される。

【0007】

また、本発明によれば、サーバとクライアント端末とを含むネットワークシステムを利用したデータ管理方法であって、

サーバにより、クライアント端末からの利用者によるデータ格納要求を受け付ける受付工程と、

前記サーバにより、前記データ格納要求に係るデータを格納するデータサーバを選定する選定工程と、

前記サーバにより、選定した前記データサーバに、前記データ格納要求に係るデータを送信し、格納させる格納工程と、

を含むデータ管理方法が提供される。

【0008】

また、本発明によれば、通信回線を介してクライアント端末から送信された、利用者によるデータ格納要求を受け付ける受付手段と、

前記データ格納要求に係るデータを格納するデータサーバを選定する選定手段と、

選定した前記データサーバに、通信回線を介して前記データ格納要求に係るデータを送信する手段と、

を備えたことを特徴とするサーバが提供される。

【0009】

また、本発明によれば、コンピュータを、

通信回線を介してクライアント端末から送信された、利用者によるデータ格納要求を受け付ける受付手段、

前記データ格納要求に係るデータを格納するデータサーバを選定する選定手段

選定した前記データサーバに、通信回線を介して前記データ格納要求に係るデータを送信する手段、

として機能させるプログラムが提供される。

【0010】

また、本発明によれば、相互に通信回線を介して通信可能とされた統括サーバ、クライアント端末、及び、複数のデータサーバを含むデータ管理システムであって、

前記統括サーバが、

前記クライアント端末から送信された、利用者によるデータ格納要求を受け付ける受付手段と、

前記データサーバの中から、前記データ格納要求に係るデータを格納するデータサーバを選定する選定手段と、

選定した前記データサーバに、前記データ格納要求に係るデータを送信する手段と、を備え、

前記データサーバが、

前記統括サーバから送信された前記データを格納する手段を備えたことを特徴とするデータ管理システムが提供される。

【0011】

【発明の実施の形態】

以下、本発明の好適な実施の形態について、図面を参照して説明する。

<システムの構成>

図1は、本発明の一実施形態に係るデータ管理が実現可能なネットワークシステムの概略図である。

【0012】

このネットワークシステムでは、アプリケーションサーバ群11と、クライアント端末群12と、が各種の通信回線から構成されるインターネット等のネットワーク10を介して通信可能に接続されている。また、本実施形態では、ネットワーク10に、災害情報を提供する災害情報データベース（サーバ）13が接続されている。

【0013】

このネットワークシステムは、主として、アプリケーションサーバ群11により、ユーザが所有する種々のデータ（以下、単にユーザデータともいう。）を代行管理するサービスを提供するものである。

【0014】

アプリケーションサーバ群11には、本実施形態のデータ管理サービスを主として実現する統括サーバ111と、ユーザが所有するデータを格納するための複数のデータサーバ112と、が含まれる。図1では、データサーバ112を例示的に2つだけ図示しているが、実施の態様によりそれ以上のデータサーバ、又は、単一のデータサーバが存在し得ることは言うまでもない。

【0015】

一方、クライアント端末群12には、リモートプリンタ121と、有線端末であるパソコン122と、無線端末である携帯電話123と、が含まれる。パソコン122又は携帯電話123には、デジタルカメラ125を接続することができ、デジタルカメラ125でユーザが撮影した画像のデータをネットワーク10へ送信することができる。

【0016】

統括サーバ111及びデータサーバ112は、汎用的なサーバコンピュータから構成することができる。

【0017】

特徴的な構成として、統括サーバ111は、ユーザデータを暗号化するための複数種類の暗号化アルゴリズムプログラムを実行可能に記憶しており、また、会員プロファイル、データサーバプロファイル、及び、格納データリスト、を記憶

している。

【0018】

会員プロフィールには、本実施形態のデータ管理サービスの提供を受けるユーザ（会員）に関する情報が記録されている。図5は、会員プロフィールの一例を示す図である。図5の会員プロフィールには、各会員を特定するIDNo.と、会員認証のためのパスワードと、会員の登録住所と、が記録されている。登録住所は、会員が会員登録時に任意に設定するもので、会員の住所、勤務先等が挙げられる。この登録住所は、ユーザが本システムにおいて格納を希望するデータサーバの選定の基準となり得るものである。なお、図示していないが、会員プロフィールには、例えば、その会員の電子メールアドレス等も記録される。

【0019】

データサーバプロフィールには、本実施形態においてユーザデータの格納先となるデータサーバに関する情報が記録されている。図6は、データサーバプロフィールの一例を示す図である。図6のデータサーバプロフィールには、各データサーバを特定するアドレスと、成りすまし等の不正サーバを排除するための認証のための認証パスワードと、そのデータサーバの設置場所を示す設置住所と、が記録されている。設置住所は、ユーザデータを格納するデータサーバを選定する際に用いられる。

【0020】

格納データリストには、各会員毎のユーザデータの格納情報が記録されている。図7は、格納データリストの一例を示す図である。図7の格納データリストには、各会員を特定するIDNo.と、各ユーザデータを特定するユーザデータのファイル名と、ユーザデータの格納先のデータサーバを特定する格納先サーバアドレスと、後述するユーザデータの暗号化に関する情報である暗号化アルゴリズム及び暗号化キーと、ユーザデータの格納日と、が記録されている。

【0021】

また、各データサーバ112には、格納したユーザデータに対する会員からの送信要求に対応するように、上述した会員プロフィールを記憶している。また、統括サーバ111との間で認証を行うために、データサーバプロフィールに記録

された認証パスワードも記憶している。

【0022】

次に、図8は、デジタルカメラ125の機能ブロック図である。

【0023】

デジタルカメラ125は、撮像部1401と、撮像部1401にて撮像された画像を電子データ化する画像処理部1402と、データを所定の暗号化アルゴリズム・暗号化キーに基づいて、暗号化／復号化する暗号処理部1403と、電子画像データを可視画像データに変換する出力制御部1404と、デジタルカメラ125の制御を司る制御CPU1405と、電子データ化された画像を蓄積・保存する着脱メモリユニット1406と、図1のパソコン122や携帯電話123といったクライアント端末とのローカルリンクの通信を司る通信インタフェース1407と、デジタルカメラ125の制御プログラムを格納するメモリ1408と、図1のICカード124との間の通信を司るICカードインタフェース1409と、出力制御部1404にて変換された可視画像データに基づく画像を表示するディスプレイ1410と、を備える。ICカード124は、ユーザが、本実施形態のデータ管理サービスを受け得る会員であるか否か等を識別するためのユーザ識別モジュールとして機能するものである。

【0024】

次に、図9は、図1のリモートプリンタ121の機能ブロック図である。

【0025】

リモートプリンタ121は、スキャナやパソコン等からのローカルな画像データを受け付けるローカル入力インタフェース1501と、入力された画像データを所定のフォーマットに変換する画像処理部1502と、データを所定の暗号化アルゴリズム・暗号化キーに基づいて、暗号化／復号化する暗号処理部1503と、画像データを可視画像データに変換すると共に、プリンタエンジン1510をコントロールする出力制御部1504と、リモートプリンタ121の制御を司る制御CPU1505と、電子データ化された画像を蓄積・保存する着脱メモリユニット1506と、図1のネットワーク10との通信を司る通信インタフェース1507と、リモートプリンタ121の制御プログラムを格納するメモリ15

08と、ICカード124との間の通信を司るICカードインタフェース1509と、出力制御部1504のコントロールに従い印刷を行うプリンタエンジン1510と、を備える。

【0026】

次に、図10はICカード124の論理情報記憶階層モデルの一例を示す図である。本実施形態では、このICカード124として、ISO7816に準拠した端子付スマートカードを想定している。

【0027】

この階層モデルでは、ICカード124の論理ファイルの構造の最上位階層であるMF(Master File)1601と、MF1601の直下に存在する最上位DF(Dedicate File)1603及び1604と、最上位DF1603及び1604に関する情報を格納する要素ファイルである最上位EF(Elementary File)1602と、がある。本実施形態では、最上位のDF(サービス提供者用DF)識別用のアプリケーションIDをサービス提供者毎にユニークな値を割当て、前記DF(1603, 1604)の下位にサービス提供者が提供するサービスメニュー毎にユニークなアプリケーションIDが割当てられるDF(サービスアプリケーションDF)のうち、本実施形態のユーザデータ格納サービスに関わるDF(1605, 1606)の下位に本アプリケーションで利用される各種情報(本実施形態においては、各サービス提供者の前記ユーザデータ格納サービス毎に割り当てられている、データ格納サーバアドレスや前記データ格納サーバ上に格納されたデータを復号化する際に必要な暗号鍵情報等)が格納(1607~1612)されるファイル階層構造を採用している。

【0028】

また、複数のサービス提供者のアライアンスにより、各サービス提供者が同意した情報フォーマットを用いるのであれば、前記ユーザデータ格納サービスに関わるDF(1605, 1606)を単一のDFとし、前記ユーザデータ格納サービスとして単一のアプリケーションIDを割当てたDFを最上位DFに採用しても、本実施形態のファイル階層構造を採用することも可能である。

【0029】

なお、このICカード124により実現されるファイル階層構造的な情報記憶機能は、リモートプリンタ121、パソコン122、若しくは、携帯電話123に直接組み込むことにより、ICカード124を用いない態様でも、本実施形態が実現可能であることは言うまでもない。

【0030】

以下、係る構成からなるシステム上で実行されるデータ管理処理について説明する。

＜ユーザデータの格納＞

ユーザが、クライアント端末（ここでは携帯電話123とする。）を介してデジタルカメラ125で撮影した画像の画像データを、データサーバ112へ格納する場合の処理について説明する。図2は、係るデータ格納処理を示すフローチャートである。

【0031】

ステップS1では、携帯電話123により統括サーバ111にアクセスして、デジタルカメラ125で撮影した画像データの格納要求を送信する。本実施形態では、予め登録した会員に対してのみデータ管理サービスを提供するので、格納要求には、ユーザのIDNo. 及びパスワードといった会員であるか否かを認証するための情報が含まれる。これらの情報は、ICカード124から取得される。

【0032】

ステップS11では、統括サーバ111が、携帯電話123からの格納要求に対応して受付処理を実行する。この受付処理において、統括サーバ111は、図5に示した会員プロフィールを参照して、格納要求が正規の会員により成されたものか否かを判定するユーザ認証処理を行う。ユーザ認証に成功すれば、会員が格納を要求する画像データの転送を許可し、失敗すれば、携帯電話123との間の通信を切断することとなる。

【0033】

ユーザ認証に成功した場合、ステップS2において、携帯電話123からデジタルカメラ125で撮影した画像データが統括サーバ111に送信される。

【0034】

次に、ステップS12において、統括サーバ111は、受信したユーザデータを一時的に格納する。この際、受信したユーザデータのチェックサム等により転送中のデータ誤りの有無を判定し、データ誤りを検出した際には、携帯電話123にユーザデータの再送を要求するようにすることもできる。

【0035】

ステップS13において、統括サーバ111は、災害情報データベース13にアクセスして災害情報を要求する。これに対して、災害情報データベース13では、災害情報を統括サーバ111に送信する（ステップS41）。

【0036】

災害情報としては、例えば、台風、地震といった災害の予知情報が含まれ、統括サーバ111では、各地域毎の災害発生予想率を調べる。このような災害発生予想率は、例えば、気象庁や民間業者がネットワーク上で提供する災害情報のほか、損害保険会社等が管理している損害保険（火災保険、地震保険等）の地域毎の料率情報から調べることも可能である。

【0037】

また、本実施形態では、統括サーバ111が会員からの格納要求がある度に、災害情報を取得することとしたが、定期的にこの情報を取得しておき、統括サーバ111内に格納することで、ステップS13の処理を省略するようにすることもできる。

【0038】

次に、ステップS14では、統括サーバ111が、図6のデータサーバプロファイルを参照して、データサーバ112の中からユーザデータを格納するデータサーバを選定する。本実施形態では、2つのデータサーバを選定することとする。このために、まず、統括サーバ111は、格納要求をしたユーザ（会員）の会員プロフィールを参照し、その登録住所を取得する。

【0039】

次に、統括サーバ111は、データサーバプロファイルを参照し、ユーザの登録住所以外の都道府県、市町村といった地域又は場所に設置されたデータサーバ

を一つ選定し、これをユーザデータの格納先のデータサーバ（A）とする。次に、この全てのデータサーバ112の中から、先に調べた災害発生発生予想率が、予め定めた閾値以下の地域又は場所に所在するデータサーバを一つ選定し、これをユーザデータの格納先のデータサーバ（B）とする。

【0040】

なお、この場合、統括サーバ111は、データサーバの選定後に、当該データサーバにアクセスし、データサーバプロファイルを参照して選定したデータサーバA及びBの認証を行い、これらが成りすまし等の不正サーバでないことの確認を行うようにしてもよい。このようなデータサーバの認証を行った結果、選定したデータサーバが不正サーバであった場合、そのデータサーバの選定を取消して、再度データサーバの選定を行い、また、その不正サーバを記録しておいて、以降のデータサーバ選定時には、その優先順位を低くするようにしてもよい。このようなサーバの認証を行うことにより、システム及びサービスの信頼性を向上することができる。

【0041】

次に、本実施形態では、後で説明するように、データサーバA及びBへ、それぞれ異なる暗号化が施されたユーザデータを格納するので、それぞれの暗号化／復号化のための暗号化アルゴリズム及び暗号化キーを定める。本実施形態では、2つのデータサーバへユーザデータを格納するので、2種類の暗号化アルゴリズムを用いて、2種類の暗号化キーを用いるか、若しくは、1種類の暗号化アルゴリズムを用いて2種類の暗号化キーを用いることとなる。

【0042】

次に、ステップS15では、統括サーバ111が携帯電話123へ、格納されるユーザデータを特定するためのファイル名、ユーザデータの格納先であるデータサーバA及びBの各アドレス、暗号化アルゴリズムの情報、及び、暗号化キー、格納条件を送信し、併せて、図7に示した格納データリストが更新される。なお、この格納条件の送信は、ユーザデータをデータサーバに格納した後に行ってもよいことはいうまでもない。

【0043】

ステップS3では、携帯電話123が、統括サーバ111から送信された格納条件をデジタルカメラ125に装着されているICカード124に格納する。格納後、携帯電話123と統括サーバ111との間の通信は切断される。

【0044】

ステップS16では、統括サーバ111が、ユーザデータの暗号化を行う。暗号化は、ステップS14で定めた暗号化アルゴリズム、暗号化キーに従って、各データサーバA及びBについて、別々の暗号化方式で行う。

【0045】

ステップS17では、統括サーバ111が、選定されたデータサーバA及びBに順にアクセスして、暗号化されたユーザデータを、データサーバA及びBへそれぞれ送信する。ステップS21及びS31では、データサーバA及びBが、統括サーバ111から送信されたユーザデータを格納する。格納後、処理が終了する。

【0046】

このように本実施形態では、ユーザが所有する画像データ等のデータをネットワーク上のデータサーバ112に格納することができるので、当該データをユーザの端末に格納しておく必要がなく、そのメモリを有効に活用できる。

【0047】

また、ユーザがデータ格納場所を指定するための特段の操作を行なわなくても、ユーザデータが、ユーザの登録住所とは異なる場所に設置されたデータサーバか、若しくは、災害発生率の低い場所に設置されたデータサーバに格納されるので、ユーザの登録住所が災害に被災した場合であっても、大事なユーザデータを保護することができる。

＜格納データの取得＞

次に、データサーバ112に格納されたユーザデータをクライアント端末（ここではリモートプリンタ121とする。）で取得する場合の処理について説明する。図3は、係るデータ取得処理を示すフローチャートである。この処理は、ユーザがリモートプリンタ121にICカード124を装着し、リモートプリンタ121に対して、ユーザデータを特定した上で、そのデータの取得を指示するこ

とにより開始される。

【 0 0 4 8 】

ステップ S 1 0 1 では、リモートプリンタ 1 2 1 が IC カード 1 2 4 から指示のあったユーザデータが格納されているデータサーバ 1 1 2 のアドレス、暗号化キー、暗号化アルゴリズム情報といった格納条件、及び、会員の ID N o. 、パスワードを読み出す。ステップ S 1 0 2 では、リモートプリンタ 1 2 1 が、ステップ S 1 0 1 で読み出したアドレスのデータサーバ (1 1 2) にアクセスし、IC カード 1 2 4 から読み出した会員の ID N o. 、パスワードと共にファイル名を指定してユーザデータの送信要求を送信する。

【 0 0 4 9 】

ステップ S 1 1 1 では、リモートプリンタ 1 2 1 からの送信要求に対して、データサーバ (1 1 2) が受付処理を行う。この受付処理において、データサーバ (1 1 2) は、送信要求が正規の会員により成されたものか否かを判定するユーザ認証処理を行う。ユーザ認証に成功すれば、送信要求のされたユーザデータの転送を許可し、失敗すれば、リモートプリンタ 1 2 1 との間の通信を切断することとなる。ユーザ認証に成功した場合、ステップ S 1 1 2 において、データサーバ (1 1 2) からリモートプリンタ 1 2 1 へユーザデータが送信され、リモートプリンタ 1 1 2 との間の通信が切断される。リモートプリンタ 1 2 1 は、データサーバ (1 1 2) からのユーザデータを受け取り、チェックサム等により転送されたユーザデータの正当性の判定を行い、エラーを検出した際には当該ユーザデータの再送を要求するようにすることもできる。

【 0 0 5 0 】

ステップ S 1 0 3 では、リモートプリンタ 1 2 1 が、暗号処理部 1 5 0 3 により、転送されたユーザデータを、IC カード 1 2 4 から読み出した暗号化キー、暗号化アルゴリズムを用いてユーザデータを復号化する。ステップ S 1 0 4 では、復号化したユーザデータを印刷出力して処理が終了する。

【 0 0 5 1 】

以上により、各ユーザは、データサーバ 1 1 2 に格納されたユーザデータを、取得することができる。なお、本実施形態では、クライアント端末から直接デー

タサーバ112にアクセスして、格納されたユーザデータの送信要求を行うようにしたが、統括サーバ111を介して、ユーザデータの送信要求を行うようにしてもよい。

＜格納データの改竄チェック＞

本実施形態では、データサーバ112に格納されたユーザデータのセキュリティを向上するために、格納されたユーザデータが改竄されていないか否かを統括サーバ111が定期的にチェックする。

【0052】

統括サーバ111は、図7の格納データリストに記録された各データの格納日を定期的に（例えば、毎日）チェックし、格納日から数日、数週間若しくは数ヶ月を経過したユーザデータの改竄をチェックすべく、以下の処理を実行する。図4は、係る改竄チェック処理を示すフローチャートである。

【0053】

ステップS201では、統括サーバ111が、チェックの対象となるユーザデータが格納されているデータサーバA及びBに順次アクセスし、ユーザデータの転送要求を送信する。

【0054】

ステップS211及びS221では、データサーバA及びBが、統括サーバ111からのデータ転送要求に対応して受付処理を実行する。ステップS212及びS222では、データサーバA及びBが統括サーバ111へユーザデータを送信する。

【0055】

なお、これらの処理において、統括サーバ111により、データサーバの認証を行い、これらが成りすまし等の不正サーバでないことの確認を行うようにしてもよい。このようなデータサーバの認証を行った結果、選定したデータサーバが不正サーバであった場合、不正サーバと判定された回数を記録しておき、予め定めた閾値以上となった場合には、クライアント端末経由で会員に通知するようにしてもよい。

【0056】

次に、ステップS202では、統括サーバ111が、データサーバA及びBから送信されたユーザデータを、図7の格納データリストに記録された暗号化アルゴリズム及び暗号化キーに基づいて復号化する。

【0057】

ステップS203では、統括サーバ111が、復号化したユーザデータを比較し、一致するか否かを判定する。ユーザデータが一致している場合は処理を終了しデータサーバA及びBとの通信を切断する。一致していない場合には、ステップS205へ進み、データサーバA及びBに対して、それぞれ、転送したデータに誤りがないか否かのエラー検出処理を実行するように指示する。ユーザデータが一致しない原因としては、改竄の他、データサーバ112の動作エラー等も考えられるからである。

【0058】

ステップS213及びS214では、データサーバA及びBが、統括サーバ111の指示に従って、エラー検出処理を実行する。本実施形態では、データサーバA及びBが、それぞれ、ユーザデータが格納されたメモリのメモリスキャン（ローカルチェック）を実行し、エラーを検出し、補正可能であればエラー箇所の補正を行う。

【0059】

ステップS214及びS224では、データサーバA及びBが、それぞれ統括サーバ111に対して、エラー検出処理の結果を通知する。エラーがあった場合は、補正後のユーザデータも合わせて送信する。

【0060】

ステップS206では、統括サーバ111が、データサーバA及びBからのエラー検出の処理結果を受け取り、エラーがあったか否かを判定する。エラーがあった場合には、ステップS202へ戻って補正後のユーザデータを用いて上述した処理を実行する。エラーがなかった場合には、データサーバA又はB上で、何らかの事情により、ユーザデータが改竄されたと判定し、これをそのユーザのクライアント端末へ電子メール等により通知する（ステップS207）。また、改竄された箇所を統括サーバ111内のメモリに格納しておき、ユーザの要求に従

って、これを通知することもできる。

【0061】

以上のように、アプリケーション統括サーバ111が自律的、定期的にデータサーバ112上のデータ正当性のチェックを行なうので、会員が、データサーバ112上に格納・保管しているユーザデータの正当性（改竄がない等）を確認するための手間を大幅に軽減することが可能となる。

【0062】

なお、本発明は、複数の機器（例えばホストコンピュータ、インタフェイス機器、リーダ、プリンタなど）から構成されるシステムに適用しても、一つの機器からなる装置（例えば、複写機、ファクシミリ装置など）に適用してもよい。

【0063】

また、本発明の目的は、前述した実施形態の機能を実現するソフトウェアのプログラムコードを記録した記憶媒体（または記録媒体）を、システムあるいは装置に供給し、そのシステムあるいは装置のコンピュータ（またはCPUやMPU）が記憶媒体に格納されたプログラムコードを読み出し実行することによっても、達成されることは言うまでもない。この場合、記憶媒体から読み出されたプログラムコード自体が前述した実施形態の機能を実現することになり、そのプログラムコードを記憶した記憶媒体は本発明を構成することになる。また、コンピュータが読み出したプログラムコードを実行することにより、前述した実施形態の機能が実現されるだけでなく、そのプログラムコードの指示に基づき、コンピュータ上で稼働しているオペレーティングシステム（OS）などが実際の処理の一部または全部を行い、その処理によって前述した実施形態の機能が実現される場合も含まれることは言うまでもない。

【0064】

さらに、記憶媒体から読み出されたプログラムコードが、コンピュータに挿入された機能拡張カードやコンピュータに接続された機能拡張ユニットに備わるメモリに書込まれた後、そのプログラムコードの指示に基づき、その機能拡張カードや機能拡張ユニットに備わるCPUなどが実際の処理の一部または全部を行い、その処理によって前述した実施形態の機能が実現される場合も含まれることは

言うまでもない。

【 0 0 6 5 】

【発明の効果】

以上説明したように、本発明によれば、ユーザが所有する電子データを好適に管理することができる。

【図面の簡単な説明】

【図 1】

本発明の一実施形態に係るネットワークシステムの概略図である。

【図 2】

図 1 のネットワークシステムで実行されるデータ格納処理を示すフローチャートである。

【図 3】

図 1 のネットワークシステムで実行されるデータ取得処理を示すフローチャートである。

【図 4】

図 1 のネットワークシステムで実行される改竄チェック処理を示すフローチャートである。

【図 5】

会員プロフィールの一例を示す図である。

【図 6】

データサーバプロフィールの一例を示す図である。

【図 7】

格納データリストの一例を示す図である。

【図 8】

デジタルカメラ 1 2 5 の機能ブロック図である。

【図 9】

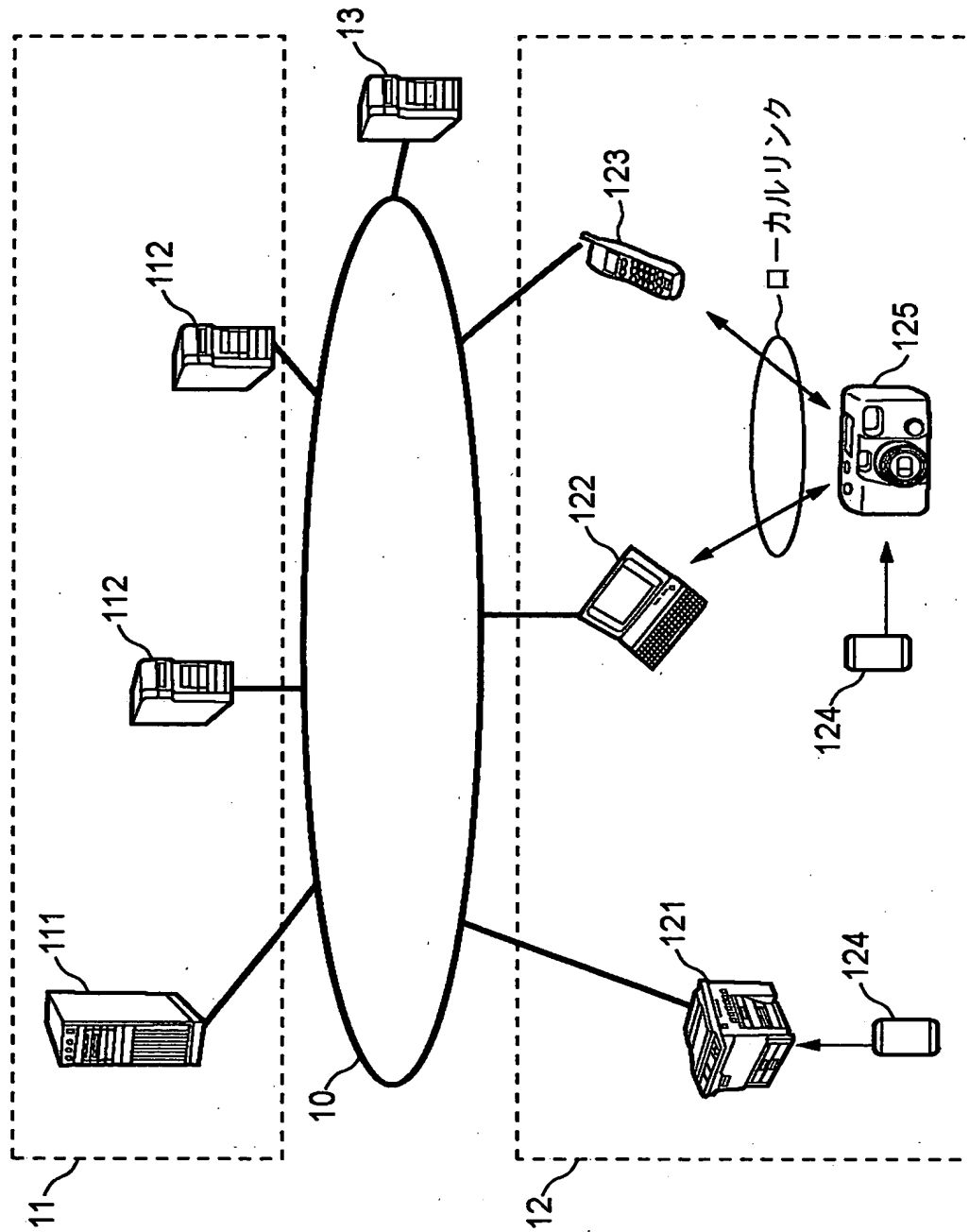
リモートプリンタ 1 2 1 の機能ブロック図である。

【図 1 0】

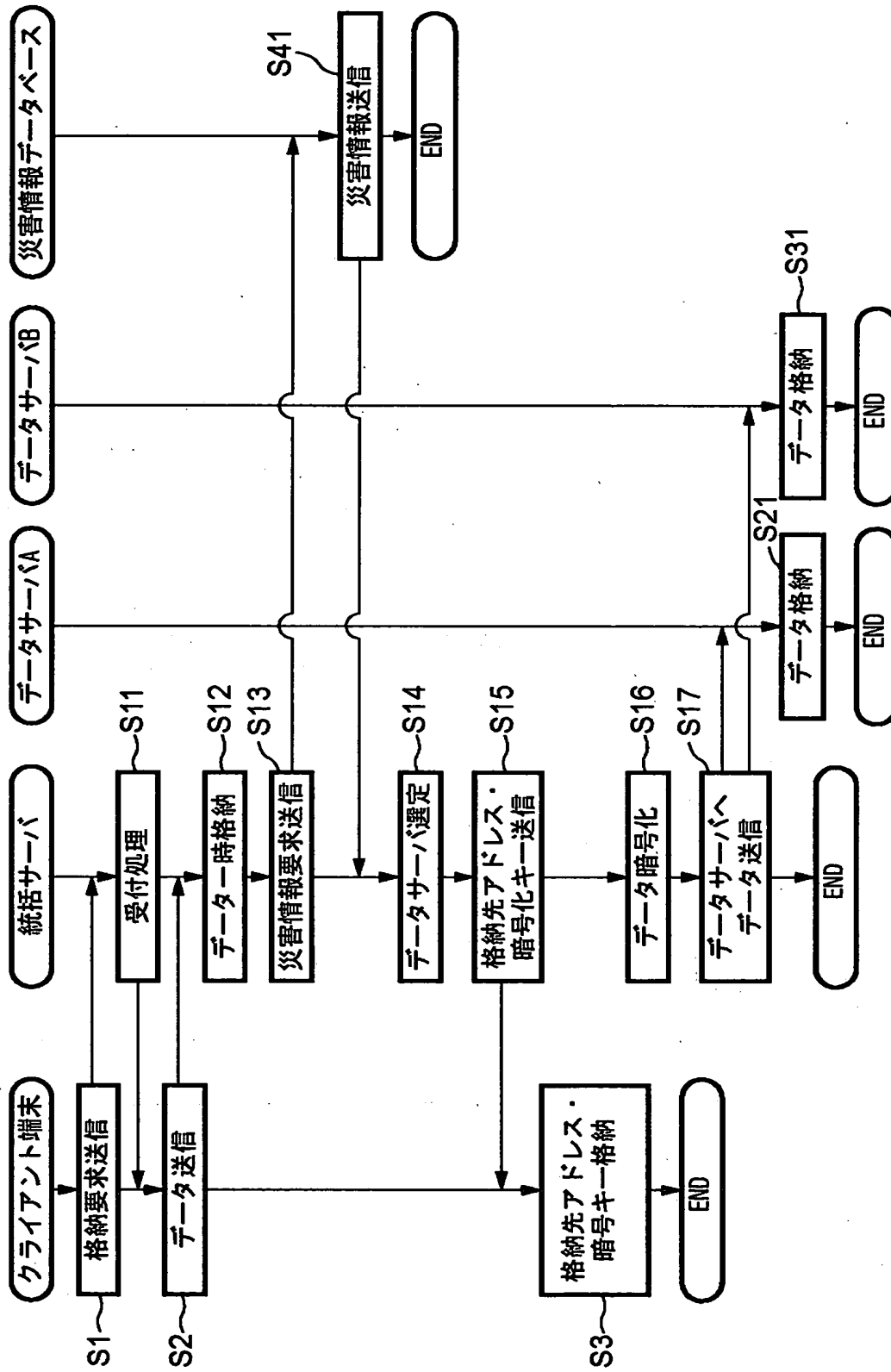
I C カード 1 2 4 の論理情報記憶階層モデルの一例を示す図である。

【書類名】 図面

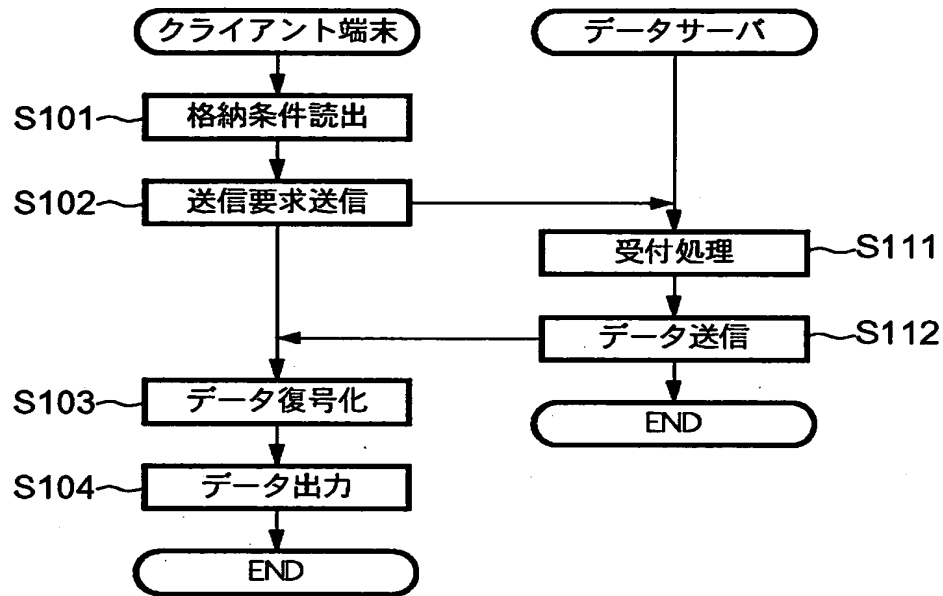
【図 1】



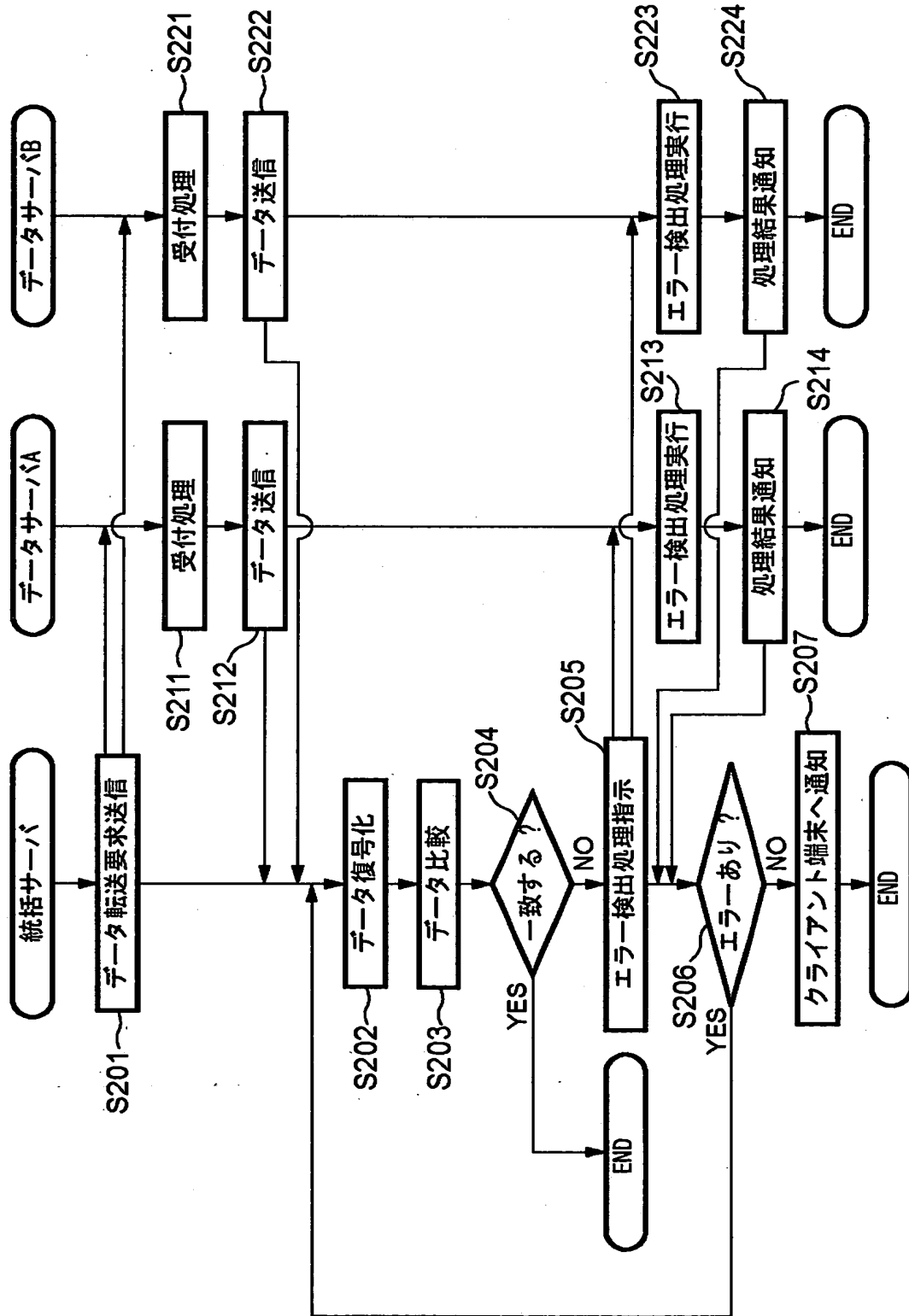
【図2】



【図 3】



【図4】



【図 5】

会員プロフィール

ID NO.	パスワード	登録住所			
A0001	aaabaa	東京都	××区	〇〇町	×〇×
A0002	bbcsed	埼玉県	〇×市	×△町	〇×〇
A0003	gghkdd	福岡県	△〇市	×〇町	△□×
...

【図 6】

データサーバプロフィール

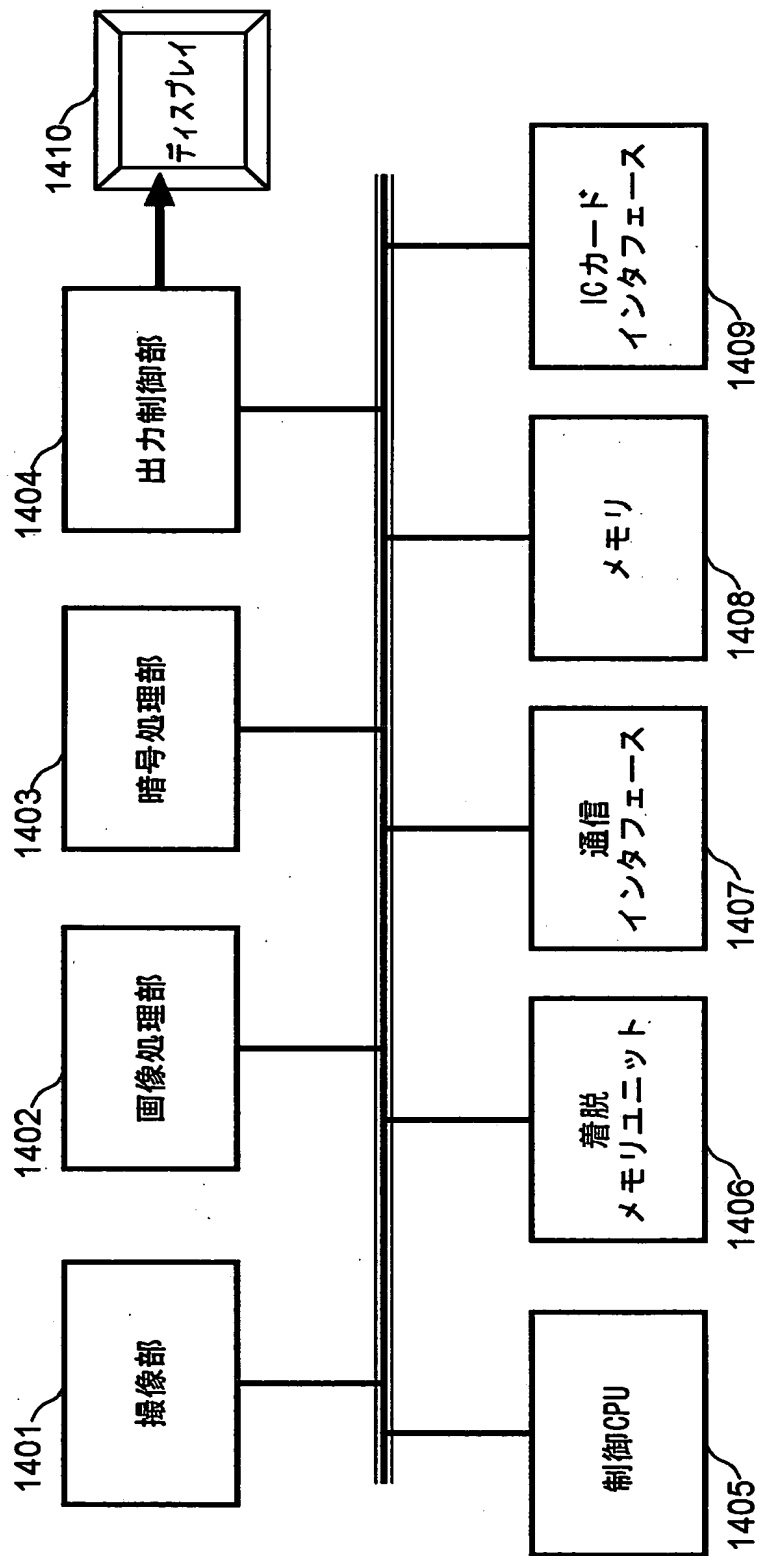
アドレス	認証パスワード	設置住所			
103.1.2.10	abaa	群馬県	××市	〇〇町	×〇×
104.2.1.30	xxbb	北海道	〇×区	×△町	〇×〇
201.2.1.05	kkgh	アメリカ	△〇州	×〇ストリート	△□×
...

【図 7】

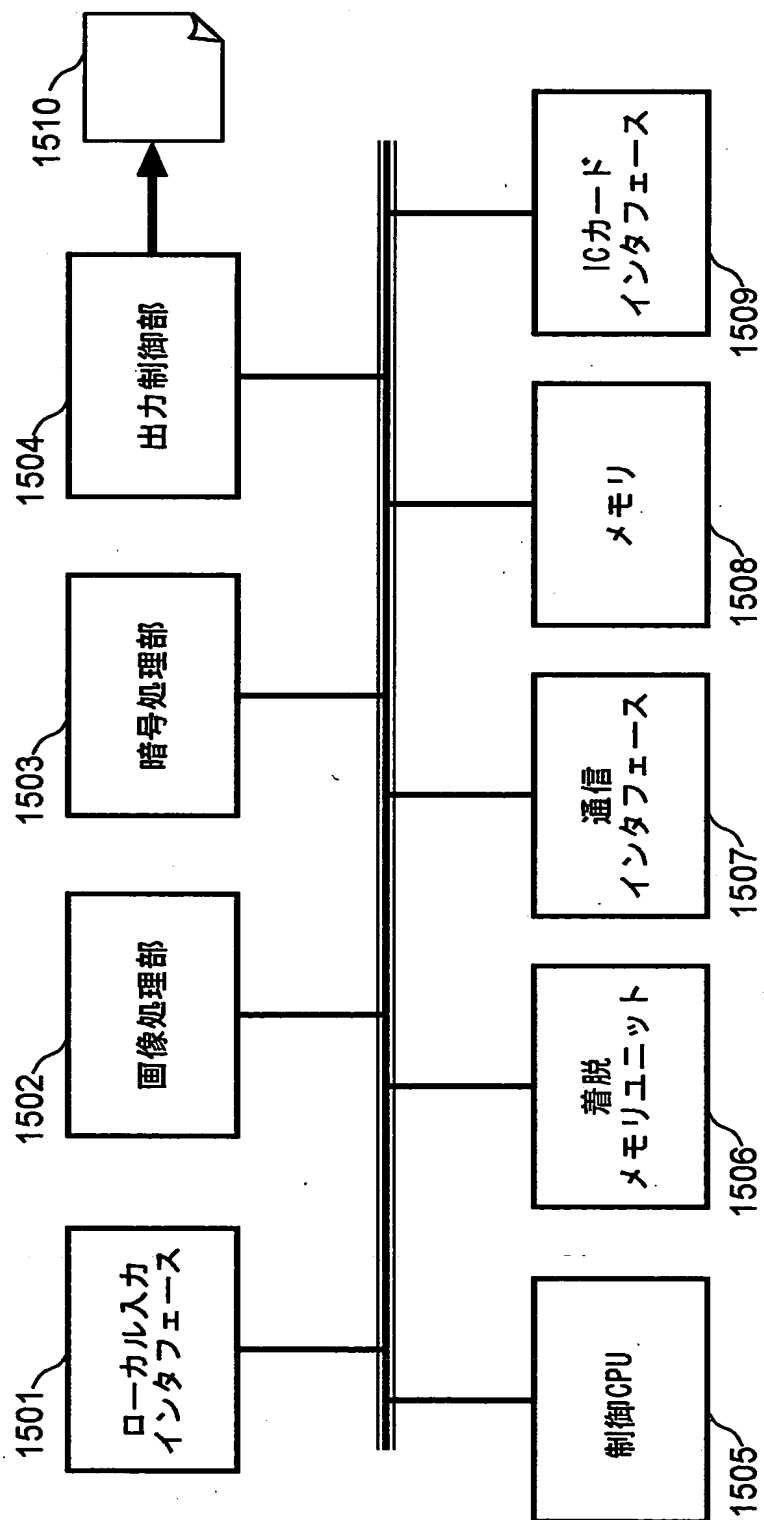
格納データリスト

ID NO.	ファイル名	格納先サーバアドレス	暗号化アルゴリズム	暗号化キー		格納日
A0001	picture 1	201.2.1.04	x x x	aba		x x 年 O 月 Δ 日
		301.5.3.51	000	xcd		
	picture 2	202.1.3.65
			
	text 1
			

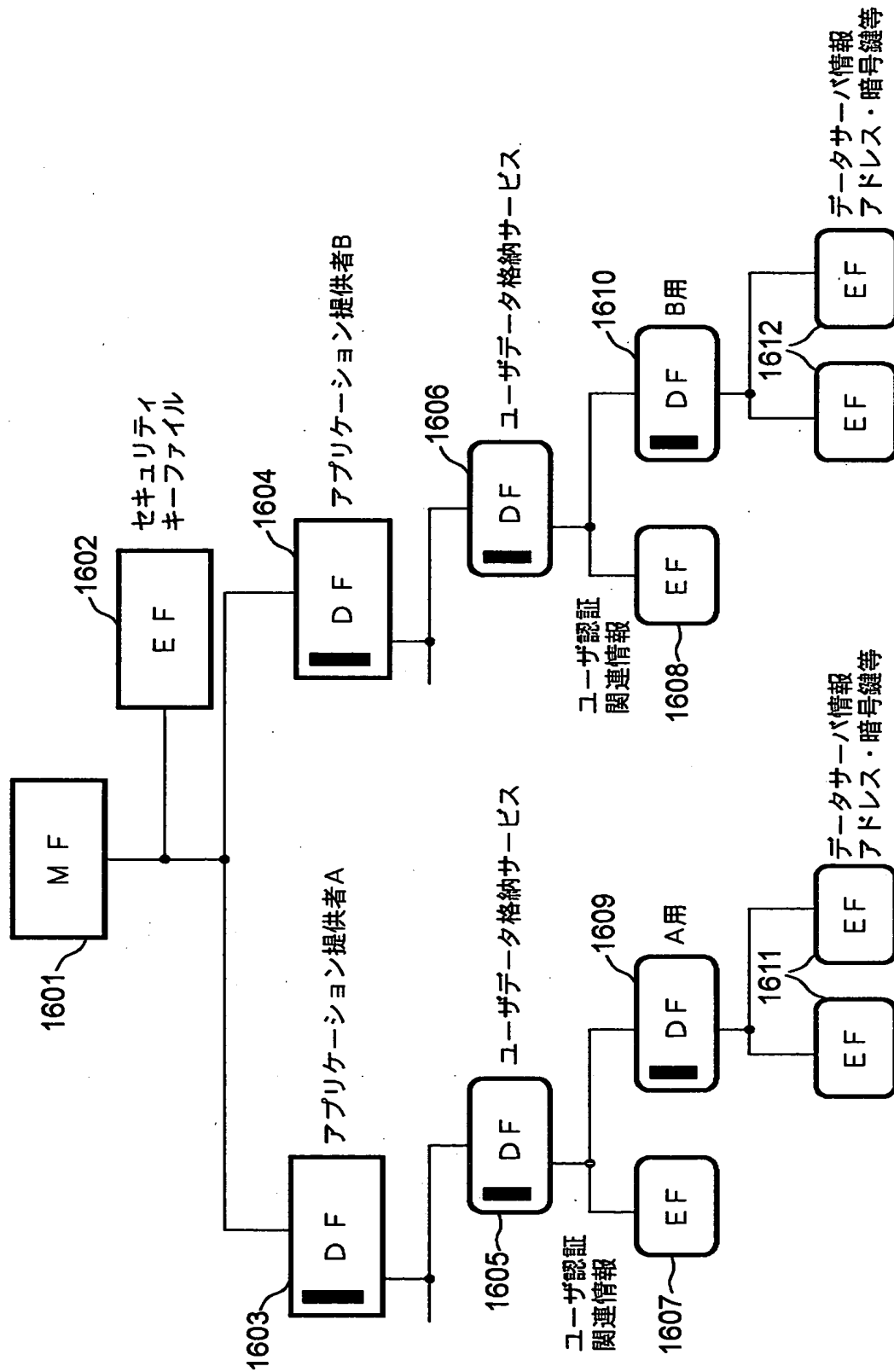
【図8】



【図9】



【図10】



【書類名】 要約書

【要約】

【課題】 ユーザが所有する電子データを好適に管理すること。

【解決手段】 サーバとクライアント端末とを含むネットワークシステムを利用したデータ管理方法であって、統括サーバにより、クライアント端末からの利用者によるデータ格納要求を受け付ける工程（S 1 1）と、統括サーバにより、予め利用者が設定した地域と一定の関係のある地域に設置されたデータサーバを選定する工程（S 1 4）と、統括サーバにより、選定したデータサーバに、前記データ格納要求に係るデータを送信し、格納させる工程（S 1 7）と、を含む。

【選択図】 図 2

出 願 人 履 歴 情 報

識別番号

[000001007]

1. 変更年月日 1990年 8月30日

[変更理由] 新規登録

住 所 東京都大田区下丸子3丁目30番2号

氏 名 キヤノン株式会社